

3

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-191402

(43)Date of publication of application : 30.07.1993

(51)Int.Cl. H04L 9/22  
G09C 1/00  
H04L 9/06  
H04L 9/14

(21)Application number : 04-003670

(71)Applicant : HITACHI LTD

(22)Date of filing : 13.01.1992

(72)Inventor : FUKUZAWA YASUKO  
TAKARAGI KAZUO  
NAKAMURA TSUTOMU  
HIRANO SHUICHI

## (54) GENERATING SYSTEM FOR ASYMMETRICAL CIPHERING KEY

## (57)Abstract:

PURPOSE: To facilitate the management and operation by generating an open key from information specific to a computer so as to register only the specific information and the open key to a center thereby reducing a verification time of the open key by the center.

CONSTITUTION: An open key of an asymmetrical ciphering key is generated from open identification information specific to a computer possessing a key or a person possessing a key. Thus, since the identification information specific to the possessor of the key or the computer possessing the key is verified from an open key of the asymmetrical ciphering key, it is not required to verify the open key with the center. Thus, the data to be verified by the center is the open key and the specific information of the key possessor or the computer possessing the key and the open key is eliminated from the data to be verified by the center.

ID情報

特許ビタト

## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平5-191402

(43)公開日 平成5年(1993)7月30日

(51)Int.Cl. <sup>5</sup>	識別記号	庁内整理番号	FI	技術表示箇所
H 0 4 L 9/22				
G 0 9 C 1/00		9194-5L		
H 0 4 L 9/06		7117-5K	H 0 4 L 9/ 04	
		7117-5K	9/ 02	Z
審査請求 未請求 請求項の数9(全 8 頁) 最終頁に続く				

(21)出願番号	特願平4-3670	(71)出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目6番地
(22)出願日	平成4年(1992)1月13日	(72)発明者	福澤 寧子 神奈川県川崎市麻生区王禅寺1099番地 株 式会社日立製作所システム開発研究所内
		(72)発明者	宝木 和夫 神奈川県川崎市麻生区王禅寺1099番地 株 式会社日立製作所システム開発研究所内
		(72)発明者	中村 勤 神奈川県川崎市麻生区王禅寺1099番地 株 式会社日立製作所システム開発研究所内
		(74)代理人	弁理士 小川 勝男
		最終頁に続く	

(54)【発明の名称】 非対称暗号鍵の生成方式

(57)【要約】

【目的】非対称鍵暗号を用いた暗号化通信に不可欠な暗号鍵の生成において、公開情報から公開鍵を生成することで、センタによる公開鍵の認証時間を短縮し、管理、運用を容易にする。

【構成】非対称暗号鍵生成プログラム205による非対称暗号鍵の公開鍵(d、n)の生成において、計算機201に固有の情報209から公開鍵(d)を生成することで、固有の情報と公開鍵(n)だけをセンタに登録する。

図1



## 【特許請求の範囲】

【請求項1】第一の公開鍵 $d$ と、秘密鍵 $e$ とが、 $e \cdot d \equiv 1 \pmod{f}$ の関係にあり、前記 $f$ の値が、第二の公開鍵を $n$ としたとき、 $n = p \cdot q$ を満たす二つの素数 $p$ 、 $q$ に対して、 $f = \text{lcm}(p-1, q-1)$ の関係（但し、 $\text{lcm}$ は最小公倍数を意味する）にあるような非対称暗号鍵の生成方式において、前記第一の公開鍵 $d$ の上位ビットに、鍵の所有者に固有の、または鍵を所有する計算装置に固有の情報を適用し、 $\text{gcd}(d, p-1, q-1) = 1$ の関係（但し、 $\text{gcd}$ は最大公約数を意味する）を満たすように、前記公開鍵 $d$ の下位ビットを調整することを特徴とする非対称暗号鍵の生成方式。

【請求項2】請求項1において、前記第一の公開鍵 $d$ の上位ビットに、鍵の所有者に固有の、または鍵を所有する計算装置に固有の情報と、前記第二の公開鍵 $n$ の情報をハッシュ処理で変換した結果とを結合して適用し、前記秘密鍵 $e$ と、前記素数 $p$ 、 $q$ との上記の関係を満たすように、前記公開鍵 $d$ の下位ビットを調整する非対称暗号鍵の生成方式。

【請求項3】請求項1または2において、前記第一の公開鍵 $d$ の上位ビットとして生成された値のうち、所定のビット数の値に応じて、予め設定されている比較的小さな素数を第一の公開鍵 $d$ として決定する非対称暗号鍵の生成方式。

【請求項4】請求項1、2または3において、生成された前記第二の公開鍵 $n$ は、 $n$ の下位一ビットを取り除いた $n-1$ ビット長の $n'$ を前記第二の公開鍵 $n$ として、予めシステムに設定されているセンタによって、センタの秘密鍵で、暗号化される非対称暗号鍵の生成方式。

【請求項5】前記第一の公開鍵 $n$ と、 $n = p \cdot q$ を満たす二つの素数 $p$ 、 $q$ を秘密鍵 $(p, q)$ とし、第二の公開鍵 $b$ が、 $0 \leq b < n$ の関係を満たすような非対称暗号鍵の生成方式において、前記第二の公開鍵 $b$ に、鍵の所有者に固有の、または鍵を所有する計算装置に固有の情報を適用することを特徴とする非対称暗号鍵の生成方式。

【請求項6】請求項5において、前記第二の公開鍵 $b$ に、前記鍵の所有者に固有の、または鍵を所有する前記計算装置に固有の情報と、前記第一の公開鍵 $n$ の情報をハッシュ処理で変換した結果とを結合して適用し、前記公開鍵 $n$ との関係を満たすように、前記第二の公開鍵 $d$ を生成する非対称暗号鍵の生成方式。

【請求項7】請求項1、2、3、4、5または6において、前記固有の情報として、利用者毎の識別情報や、計算機に予め設定されている固有の製造番号や通信アドレスを用いる非対称暗号鍵の生成方式。

【請求項8】請求項1、2、3、4、5、6または7において、前記計算機毎に固有の情報や前記鍵の所有者の識別情報を、計算機製造時に計算機内蔵ROMに書き込み、再設定ができない計算機である非対称暗号鍵の生成方式。

【請求項9】請求項1、2、3、4、5、6または7において、非対称暗号鍵生成部、および前記記憶手段は、前記計算機に着脱可能な回路装置により構成される非対称暗号鍵の生成方式。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、公開の固有情報を非対称暗号鍵の公開鍵として利用するものであり、非対称暗号鍵の生成方式に関する。

## 【0002】

【従来の技術】通信ネットワークを介して、会議や種々の取引を電子的に行うビジネス通信の時代が始まり、情報セキュリティの必要性は増大しつつある。情報セキュリティを確保するための暗号技術の一つであるRSA暗号方式やRABIN暗号方式等の非対称暗号鍵暗号方式は、データ保護だけでなく、相手認証の機能を持つことから有用な暗号方式と考えられている。（IDベース鍵生成機能の例：コーンフェルダー（Kohnfelder）の方法 出典：（株）昭昇堂発行、辻井重男、笠原正雄編著、「暗号と情報セキュリティ」pp94～）まず、RSA暗号化鍵、復号化鍵の生成の基本手順を示す。

【0003】ステップ1：十分大きな素数 $p$ 、 $q$ をランダムに選ぶ。 $p$ 、 $q$ は秘密にしておく。

【0004】ステップ2： $p \cdot q$ の積を $n$ とする。

【0005】ステップ3： $f = \text{lcm}(p-1, q-1)$ とし、 $\text{gcd}(d, f) = 1$ となる、 $f$ と互いに素な整数 $d$ をランダムに取出す。

【0006】ここで、 $\text{lcm}(x, y)$ は、 $x$ と $y$ の最小公倍数、 $\text{gcd}(x, y)$ は、 $x$ と $y$ の最大公約数を示す。

【0007】ステップ4： $f$ を法として、 $e \cdot d \equiv 1 \pmod{f}$ となる、 $d$ の逆数 $e$ を定める。

【0008】上記の手順で暗号化鍵 $(e, n)$ 、復号化鍵 $(d, n)$ が生成される。

【0009】暗号化では、平文 $M$ を $0 \sim (n-1)$ までの間の整数 $C$ に変換し、復号化では、暗号文 $C$ を平文 $M$ に変換する。

【0010】暗号化

【0011】

【数1】

$$C \equiv M^e \pmod{n}$$

【0012】復号化

【0013】

【数2】

$$M \equiv C^d \pmod{n}$$

【0014】これは $\pmod{n}$ において、積を何度も繰り返すと元に戻るという周期性に依存したアルゴリズムである。RSA暗号方式では、暗号化鍵と復号化鍵は一对をなしており、 $(e, n)$ で暗号化されたものは $(d, n)$ でしか復号化することができず、しかも $n$ の

値が五百ビット程度の長さを持つ場合には、 $(d, n)$  から  $(e)$  を求めることは、 $n$  の素因数を知らなければ計算量的に大変困難であるという性質を持つ。

【0015】RSA暗号方式を用いて秘密通信を行う場合は、暗号化鍵を公開し、復号化鍵を秘密管理する。また、逆にデジタル署名を行う場合、暗号化鍵を秘密管理し、復号化鍵を公開にする。

【0016】さて、名前や住所といった公開の識別情報(ID)そのものが、そのまま公開の暗号鍵(公開鍵)としての役目を果たすことができれば、公開鍵から鍵の所有者を認証することができるので鍵管理は非常に容易になる。この考え方は1978年頃から提案されてきている。しかし、前述したように、公開の識別情報を非対称暗号鍵暗号方式の公開鍵としてそのまま用いることは、公開の識別情報が秘密鍵との関係を満たすとは限らないので、実現できない。そこで、従来例で示されるようなIDを用いた非対称暗号鍵証明配送方式が提案されている。これを以下に示す。

【0017】(1) まず、図9に示すように、ユーザAはユーザAの公開情報(IDA)と自身の公開鍵( $d_A, n_A$ )を鍵管理機関であるセンタに登録する。

【0018】(2) センタは、センタの秘密鍵( $S_c$ )で暗号化したお墨付きの(センタによって認証された)ユーザAの公開鍵をユーザAに渡す。

【0019】ユーザAのお墨付き公開鍵:  $RSAS_c(ID_A, d_A, n_A)$

(3) 次に、図10に示すように、ユーザAと暗号通信を行いたいユーザBは、お墨付きのユーザAの公開鍵をユーザAより受取り、センタの公開鍵( $P_c$ )で復号化する。

【0020】 $RSAP_c(RSAS_c(ID_A, d_A, n_A))$

(4) 復号化した結果、ユーザAのIDAが正しい公開情報であることを確認できたら、公開鍵( $d_A, n_A$ )も正しいものであるとし、以下、公開鍵( $d_A, n_A$ )でメッセージを暗号化し、ユーザAと暗号通信を行なう。

【0021】このようにすれば、公開の識別情報から公開鍵を生成していないので、公開鍵から相手を認証することはできないが、公開の識別情報と公開鍵の関係をセンタによって認証(保証)されたことになる。

【0022】

【発明が解決しようとする課題】Kohnfelderの非対称暗号鍵証明配送方式は、安全性の面からも有効であると考えられている。しかし、センタの秘密鍵で暗号化する必要のあるデータは、利用者毎にID<sub>i</sub>、 $d_i$ 、 $n_i$ であり、三ブロックの暗号処理が必要になる。暗号化通信を行うシステムの規模をm端末と想定すると、センタはセンタの秘密鍵で $(3 \times m)$ ブロックの暗号処理を行う必要がある。従って、暗号化する必要のあるデータ長を短くし、暗号処理のブロック数を減らすことは有効とな

る。

【0023】

【課題を解決するための手段】上記問題を解決するために、本発明では次の手段を用いる。

【0024】(1) 鍵を所有する個人、あるいは鍵を所有する計算機に固有の公開の識別情報から非対称暗号鍵の公開鍵( $d$ )を生成する。

【0025】(2) 公開の識別情報から生成できない非対称暗号鍵の公開鍵( $n$ )だけを、センタの秘密鍵で暗号化し、認証する。前述したように、RSA暗号方式は、 $n$ の素因数分解の計算量的な困難さに依存した方式であることから、公開鍵( $n$ )を公開の識別情報から生成すると $n$ の素因数分解の困難性が保証されない。従って、公開鍵( $n$ )を公開の識別情報から生成することはできない。

【0026】

【作用】上記の手段により、次のような作用が生じる。

【0027】非対称暗号鍵の公開鍵( $d$ )から、鍵の所有者、あるいは鍵を所有する計算機に固有の識別情報を認証することができるので、センタによって公開鍵( $d$ )を認証する必要が無い。従って、センタによって認証すべきデータは、公開鍵( $n$ )と鍵の所有者、あるいは鍵を所有する計算機の固有情報であり、公開鍵( $d$ )をセンタによって認証すべきデータからはずすことができる。

【0028】

【実施例】図1～図8において、本方式の実施例を示す。

【0029】〈実施例1〉図2は、本実施例のシステム構成を示す図である。

【0030】センタであるホスト計算機209、ユーザの計算機(端末)201、205が通信網200を介して結ばれている。センタは鍵管理機関としての役目を果たす。ユーザ計算機201は、内部に暗号機構202を持ち、センタの公開鍵204はFD203に格納されている。同様に、ユーザ計算機205は、内部に暗号機構206を持ち、センタの公開鍵204はFD207に格納されている。ホスト計算機209は、内部に暗号機構210を持ち、ユーザの公開鍵212、213が鍵ファイル211に格納される。センタの秘密鍵214は、センタのホスト計算機だけが参照できる。

【0031】計算機(端末)201のユーザAが公開鍵をセンタ209に登録し、計算機(端末)201のユーザAと205のユーザBが暗号通信を行うまでを以下に示す。

【0032】図4は、本実施例のユーザの計算機のハードウェア構成を示す図である。

【0033】計算機201は、ディスプレイ402とキーボード403からなる。計算機201上の暗号機構202は、メモリ404とCPU406から成り、メモリ404に格納されている非対称暗号鍵生成プログラム405で、ユーザAの固有情報409から非対称暗号鍵を生成する。固有情報409とは、名

前や住所や通信アドレス等の固有の情報であり、かつ誰からも参照可能な情報である。生成された非対称暗号鍵は公開鍵と秘密鍵であり、秘密鍵はICカードR/W407を介して、ICカード408に格納し、メモリ404上にそのままの形で保管しない。公開鍵は、メモリ404上一時保管し、センタ209に登録し、センタによって認証された形でオンラインで配布するか、秘密鍵格納用のICカードとは別のICカード、あるいはF. D. 等に格納して、配布する。

【0034】以下、図5において、計算機201上で行う非対称暗号鍵生成処理(RSA暗号鍵生成処理)について示す。

【0035】ステップ501: 始め。

【0036】ステップ502: 素数 $p$ を生成する。

【0037】ステップ503: 素数 $q$ を生成する。

【0038】ステップ504: 固有情報409から、公開鍵 $d$ を生成する。

【0039】ステップ505:  $p$ ,  $q$ ,  $d$ から次ぎの条件を満たすように、鍵 $e$ ,  $n$ を生成する。

【0040】 $n = p \cdot q$ ,  $f = \text{lcm}(p-1, q-1)$   
 $e \cdot d \equiv 1 \pmod{f}$

ステップ506: 固有情報409と、公開鍵( $n$ )をセンタによって認証する。

【0041】ステップ507: 終わり。

【0042】この手順で、公開鍵 $d$ を生成する処理F(ステップ504)を図6に示す。

【0043】ステップ601: 始め。

【0044】ステップ602: 奇数乱数を生成する。

【0045】ステップ603: 固有情報409を上位ビットとし、奇数乱数を下位ビットなるように接続する。ただし、 $d' < n$ 。

【0046】 $d' = \text{固有情報} \parallel \text{奇数乱数}$

ステップ604:  $d'$ が素数であるかどうかを判定する。素数であれば、ステップ606へ進む。素数でなければ、ステップ605へ進む。

【0047】ステップ605: 奇数乱数に2を加える。ステップ603へ進む。

【0048】ステップ606:  $d'$ を $d$ として出力する。

【0049】ステップ607: 終わり。

【0050】出力される公開鍵 $d$ の形態を図1に示す。また、固有情報毎に処理Fの結果は常に一定である。

【0051】この手順で、公開鍵 $n$ をセンタに登録する処理(ステップ506)を図7で示す。

【0052】ステップ701、ステップ701': 始め。

【0053】ステップ702: 計算機201の公開鍵( $n_A$ )と固有情報( $ID_A$ )409をセンタのホスト計算機209に送る(手配送、あるいは別途暗号化して送る)。

【0054】ステップ703: ホスト計算機では、公開鍵( $n_A$ )と固有情報( $ID_A$ )をセンタ秘密鍵( $Sc$ )214を用いて、暗号機構210によってRSA暗号方式によっ

て暗号化し、センタによって認証された情報 $C$ を生成する。

【0055】 $C = \text{RSA}_{Sc}(ID_A, n_A)$

ステップ704: 公開鍵( $n_A$ )と固有情報( $ID_A$ )を鍵ファイル211のエリア212に格納する。

【0056】ステップ705: センタによって認証された情報 $C$ を計算機201のユーザAに配布する。ステップ706: 計算機201はセンタによって認証された情報 $C$ をメモリ404に格納する。ステップ707、ステップ707': 終わり。

【0057】ただし、センタによって認証された情報( $C$ )の生成を、 $C = \text{RSA}_{Sc}(ID_A, d_A, n_A)$ として、センタによって三ブロックの暗号化で行ったとしても、公開鍵( $d_A$ )から固有情報( $ID_A$ )を認証する効果がある。

【0058】次に、ユーザA(計算機201)とユーザB(計算機205)が暗号通信を行う処理を図8で示す。

【0059】ステップ801、ステップ801': 始め。

【0060】ステップ802: 計算機205に、センタによって認証された情報( $C$ )と公開鍵( $d_A$ )を配送する。

【0061】ステップ803: FD207内のセンタの公開鍵( $Pc$ )204を用いて、暗号機構206によって情報 $C$ を復号化する。

【0062】 $ID_A, n_A = \text{RSA}_{Pc}(C)$

ステップ804: 復号化結果の固有情報( $ID_A$ )が正しければ、ステップ805に進む。正しくなければ、ステップ806に進む。

【0063】ステップ805: ( $d_A, n_A$ )を用いて、暗号通信を計算機201と計算機205で行う。

【0064】ステップ806、ステップ806': 終わり。

【0065】〈実施例2〉実施例1と同様手順で、RABIN暗号化鍵生成を行う。

【0066】RABIN暗号化鍵は、二つの大きな素数 $p$ ,  $q$ を選び、その積を計算する。次に $0 \leq b < n$ になる $b$ を定める。この時、公開鍵は( $n$ ,  $b$ )であり、秘密鍵は( $p$ ,  $q$ )となる。

【0067】ステップ501': 始め。

【0068】ステップ502': 素数 $p$ を生成する。

【0069】ステップ503': 素数 $q$ を生成する。

【0070】ステップ504': 固有の情報409を鍵 $b$ とする。

【0071】ステップ505':  $p$ ,  $q$ から鍵 $n$ を生成する。

【0072】 $n = p \cdot q$ ステップ506': 終わり。

【0073】〈変形例1〉図3は、図6の処理で生成される公開鍵( $d$ )の形態の他の例を示す。公開鍵( $d$ )は、固有の情報と、公開鍵( $n$ )を一方方向性関数 $h$ (ハッシュ関数)によって処理した結果 $h(n)$ と、 $d$ を素数にするための調整ビットから成る。公開鍵( $d$ )と

( $n$ ) の組合せを確認することが可能になる。

【0074】〈変形例2〉センタのRSA暗号秘密鍵  $S_c = (e_c, n_c)$  とすると、センタでユーザの公開鍵 ( $n$ ) を認証するためには、 $n_c > n$  でなければならない。

【0075】そこで、ユーザの公開鍵 ( $n$ ) の最下位一ビットを取り除いた  $n'$  をセンタのRSA暗号秘密鍵で認証する。つまり、( $d, n'$ ) をセンタが認証する。実際に、ユーザの公開鍵 ( $d, n$ ) を用いて暗号通信を行う場合には、センタによって認証された公開鍵 ( $d, n'$ ) の  $n'$  の最下位に1を付加し、( $d, n$ ) として暗号通信を行う。これは、 $n$  が二つの素数の積であることから、奇数である。従って、最下位ビットが1であることは自明である。

【0076】この結果、 $n_c > n$ 、かつ  $n_c$  と  $n$  が同ビット長の値である場合には、センタによる認証が可能になる。

【0077】〈変形例3〉実施例1で生成された公開鍵 ( $d$ ) の所定のビット数の値に応じて、予め設定された比較的短い素数を、公開鍵 ( $d$ ) として用いる。

【0078】〈変形例4〉以上は、計算機上のプログラムによる処理を前提としているが、図5～図8の演算の一部、あるいは全部を専用ハードウェア化することで実現することもできる。

【0079】〈変形例5〉計算機固有の情報とは、計算機据付時に、端末利用ユーザによって入力されたデータを非公開の関数(時刻データ等をパラメータとして用いることで、意図的に値を生成できないような関数)で変換、生成した一意のコードや、予め計算機製造時に割当てられた固有の製造番号や、通信アドレス等を用いる。また、通信端末内のROMに製造段階で書き込んでおく。ROMに製造段階で書き込まれることによって、ユーザが意識的に書き直すことができない。

【0080】

【発明の効果】本発明により、次のような効果が得られる。

(1) センタによって認証すべきデータは、公開鍵 ( $n$ ) と鍵の所有者、あるいは鍵を所有する計算機の固有情報にすることが可能となり、公開鍵 ( $d$ ) をセンタ

によって認証すべきデータからはずすことができるので、ユーザ毎の認証すべきデータを3ブロックから二ブロック以下にすることができる。従って、暗号化通信を行うシステムの規模を  $m$  端末と想定すると、センタはセンタの秘密鍵による暗号処理を、( $3 \times m$ ) ブロックから ( $2 \times m$ ) ブロックに短縮できる。

(2) 非対称暗号鍵の公開鍵 ( $d$ ) から、計算機、あるいは個人の固有情報を認証することができる。

(3) 公開鍵 ( $d$ ) の一部に、公開鍵 ( $n$ ) の圧縮データを組み入れることで、公開鍵 ( $d$ ) と公開鍵 ( $n$ ) の組み合わせを認証することができる。

(4) ユーザの公開鍵 ( $n$ ) の最下位一ビットを取り除いた  $n'$  をセンタのRSA暗号秘密鍵で認証することで、センタのRSA暗号鍵 ( $n_c$ ) とユーザの公開鍵 ( $n$ ) が  $n_c > n$  でも、 $n_c$  と  $n$  が同ビット長の値である場合には、センタによる認証が可能になる。

【図面の簡単な説明】

【図1】生成される公開鍵 ( $d$ ) の形態の一例を示す説明図。

【図2】本発明の実施例のシステム構成を示すブロック図。

【図3】図2のシステム構成において、生成される公開鍵 ( $d$ ) の形態の他の例を示す説明図。

【図4】ユーザの計算機のハードウェア構成を示す説明図。

【図5】図4のハードウェア構成において生成される、非対称暗号鍵の生成を示すフローチャート。

【図6】図4のハードウェア構成において生成される、非対称暗号鍵の公開鍵 ( $d$ ) の生成を示すフローチャート。

【図7】非対称暗号鍵の登録を示すフローチャート。

【図8】非対称暗号鍵を用いた暗号通信を行うための前処理を示すフローチャート。

【図9】従来例を示す説明図。

【図10】従来例を示す説明図。

【符号の説明】

200…通信網、201…計算機、205…計算機、209…ホスト。

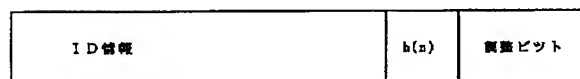
【図1】

図1

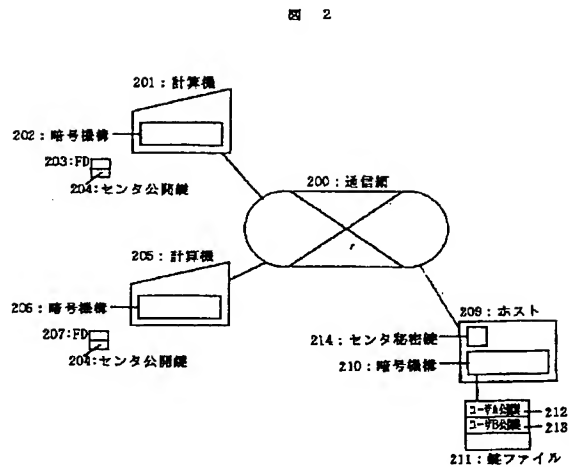


【図3】

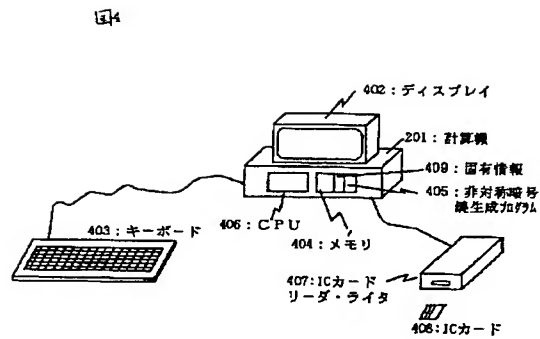
図3



【図2】

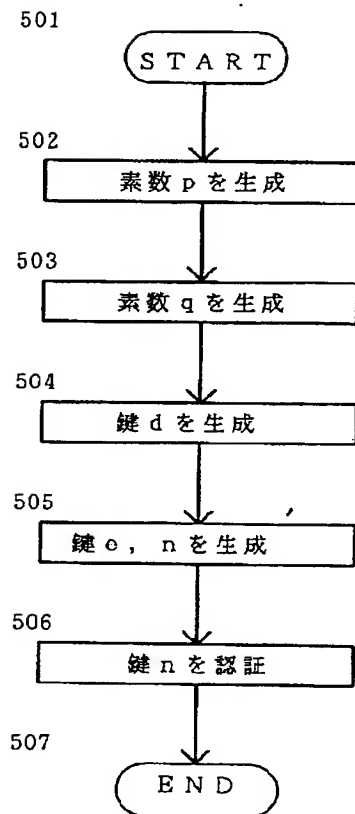


【図4】



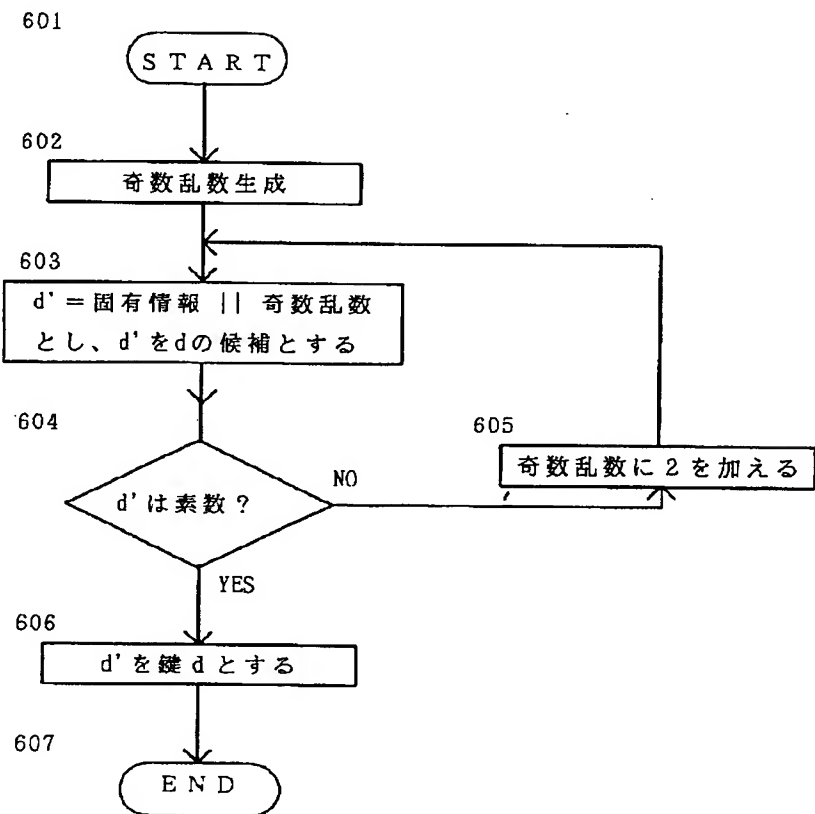
【図5】

図5



【図6】

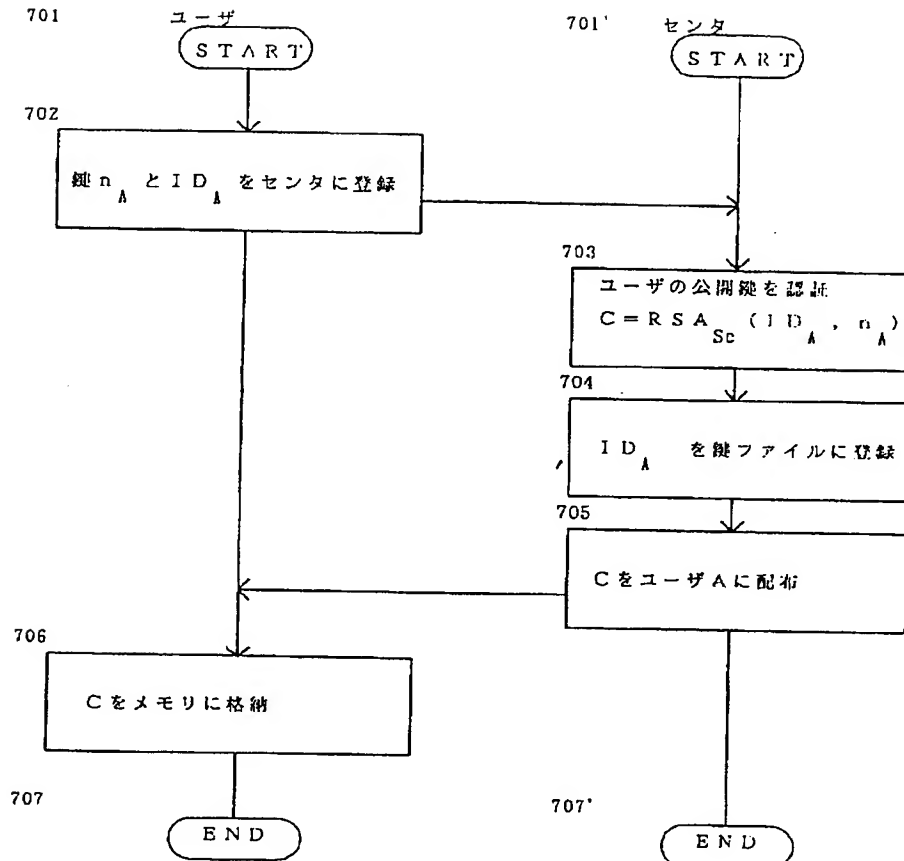
図6





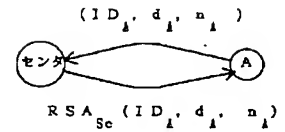
【図7】

図 7



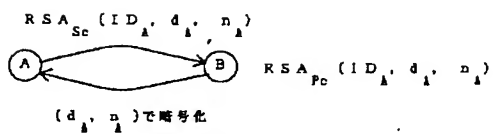
【図9】

図 9



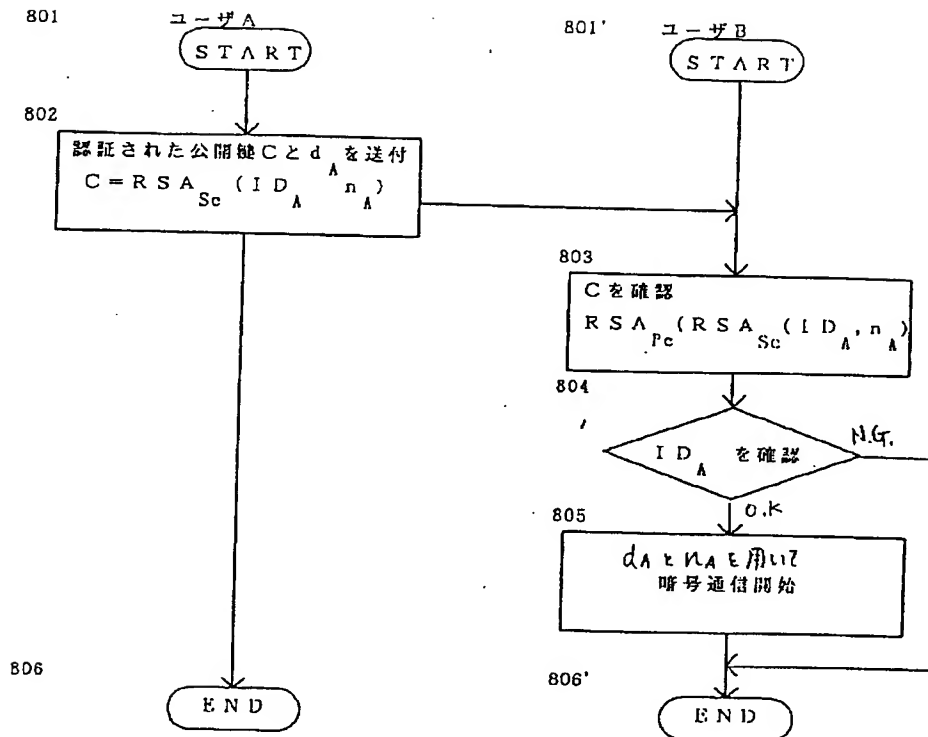
【図10】

図 10



【図8】

図8



フロントページの続き

(51) Int. Cl. 5  
H04L 9/14

識別記号 庁内整理番号

F I

技術表示箇所

(72) 発明者 平野 秀一  
神奈川県横浜市戸塚区戸塚町216番地 株  
式会社日立製作所情報通信事業部内